REMARKS

Claims 2-11, 13-19, and 22 are pending in the present application.

This Amendment is in response to the Office Action mailed April 4, 2008. In the Office Action, the Examiner rejected claims 2-11, 13, 14-19, and 22 under 35 U.S.C. §103(a). Reconsideration in light of the remarks made herein is respectfully requested.

Rejection Under 35 U.S.C. § 103

In the Office Action, the Examiner rejected claims 2-11, 14-19, and 22 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,173,400 issued to Perlman et al. ("Perlman") in view of Hugo Krawczyk "New Hash Functions for Message Authentitcation", 1988 ("Krawczyk"); and claim 13 under 35 U.S.C. §103(a) as being unpatentable over Perlman and Krawczyk as applied to claims 2-11, 14-19, and 22 above, and futher in view of U.S. Patent No. 5,703,952 issued to Taylor ("Taylor"). Applicant respectfully traverses the rejection and submits that the Examiner has not met the burden of establishing a *prima facie* case of obviousness.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *MPEP §2143, p. 2100-126 to 2100-130 (8th Ed., Rev. 5, August 2006).* Applicant respectfully submits that there is no suggestion or motivation to combine their teachings, and thus no *prima facie* case of obviousness has been established.

Perlman, Krawczyk, and Taylor, taken alone or in any combination, do not disclose or render obvious, at least, one of: (1) generating an integrity check value by the first device, comprising: (1a) extracting a selected number of bits from a pseudo-random data stream for use as coefficients of a matrix having M rows and N columns, and (1b) performing operations on both contents of the message and the coefficients of the matrix to generate the integrity check value, as recited in independent claim 2.

The Examiner argues that Perlman shows generating "an integrity check value by the first device," citing to column 4, lines 42-64. Applicant respectfully disagree and submits that Perlman merely discloses a shared secret being established using an authentication token that generates a character string which is a password based on the time of day encrypted with a secret code or a random number (Perlman, col. 4, lines 43-48), not an integrity check value, as recited in the claim. In Perlman, the character string is communicated to a local device (e.g., workstation). (Perlman, col. 4, lines 48-52). In contrast, as delineated in the claim, the integrity check value is generated by "extracting a selected number of bits from a pseudo-random data stream for use as coefficients of a matrix having M rows and N columns, and performing operations on both contents of the message and the coefficients of the matrix." Since the character string is based on the time of day encrypted with a secret code rather than being generated by performing operations on the message and the coefficients of the matrix, the character string cannot be the integrity check value.

In addition, the Examiner argues that Krawczyk shows "extracting bits randomly for use as coefficients of a matrix having M rows and N columns and performing operations to generate the integrity check value," citing to pages 301-303 (Office Action, page 3). Applicant respectfully disagrees. Krawczyk merely discloses Toeplitz matrices being characterized by having fixed diagonals (Krawczyk, page 303, Section 2.1), not performing operations on the coefficients of the matrix to generate the integrity check value, as recited in claim 2. Toeplitz matrices of dimension *n* x *m* can be used to hash messages of length *m* by multiplying the message by the matrix (Krawczyk, page 303, Section 2.1). Since hashing messages is not the same as generating the integrity check value, Krawczyk, in discussing Toeplitz matrices, does not teach or suggest this element of the claim. Furthermore, Krawczyk does not teach or suggest performing operations on both the contents of the message and the coefficients of the matrix to generate the integrity check value, as recited in claim 2.

Moreover, Applicant respectfully submits that the Examiner impermissibly uses hindsight reconstruction. While Applicant discloses in the Specification that in one embodiment of the invention "a Toplitz matrix 700 in lieu of integrity matrix 600" is used (See Specification, page 12 for further details), there is no teaching or suggestion in Krawczyk of performing operations on the coefficients of the Toeplitz matrix to generate the integrity check value since Krawczyk merely discloses using the Toeplitz matrix to hash messages. When applying 35 U.S.C. 103, the following tenets of patent law must be adhered to: (A) The claimed invention must be considered as a whole; (B) The references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination; (C) The references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention; and (D) Reasonable expectation of success is the standard with which obviousness is determined. *Hodosh v. Block Drug Col, Inc.,* 786 F.2d 1136, 1143 n.5, 229 USPQ 182, 187 n.5 (Fed. Cir. 1986). To defeat patentability based on obviousness, the suggestion to make the new product having the claimed characteristics must come from the prior art, not from the hindsight knowledge of the invention. *Interconnect Planning Corp. v. Feil*, 744 F.2d 1132, 1143, 227 USPQ (BNA) 543, 551 (Fed. Cir. 1985). "To support the conclusion that the claimed invention is directed to obvious subject matter, either the references must expressly or implicitly suggest the claimed invention or the Examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." *Ex parte Clapp*, 227 USPQ 972, 973. (Bd.Pat.App.&Inter. 1985). The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990).

With respect to the independent claim 18, as discussed above, Perlman in view of Krawczyk fails to teach or suggest at least one of: generating an integrity check value, producing the integrity check value based on a selected group of bits from a pseudo-random data stream and contents of the message.

With respect to claim 13, Applicant agrees with the Examiner that neither Perlman nor Krawczyk explicitly disclose the feature of decrypt an incoming message, computing an integrity check value for an incoming message and determining whether the incoming message is valid by comparing the computed integrity check value with the recovered integrity check value, as recited in the claim (Office Action, page 9). However, Applicant respectfully disagrees that Taylor teaches the elements of claim 13.

Taylor merely discloses an integrity function being applied to result in an integrity check value which is forwarded to the encryption processor 26 (Taylor, col. 11, lines 5-7), not determining whether the incoming message is valid by comparing the computed integrity check value with a recovered integrity check value. At the encryption processor 26, the integrity check value is appended as a message authentication code onto the end of the plain text message (Taylor, col. 11, lines 7-11). Thus, a single integrity check value is computed and subsequently appended to plain text message. Since Taylor merely discloses a single integrity check value, there is no teaching or suggestion of comparing the computed integrity check value with a recovered integrity check value.

In addition, the Examiner alleges that Taylor teaches the elements by citing to the language in column 16, lines 66-67 and in column 17, lines 1-2, which are claims 25 and 26 (Office Action, page 9). Applicants respectfully submit that it is impermissible to rely on the language in the claims as support for the teachings of Taylor. The scope of a patent's claims determines what infringes a patent; it is no measure of what it discloses. In re Benno, 768 F2d 1340, 226 USPQ 683, 686 (Fed.Cir.1985). Thus, the rejection is impermissible.

Moreover, the Examiner failed to establish the factual inquires in the three-pronged test as required by the *Graham* factual inquires. There are significant differences between the cited references and the claimed invention as discussed above. Furthermore, the Examiner has not made an explicit analysis on the apparent reason to combine the known elements in the fashion in the claimed invention. Accordingly, there is no apparent reason to combine the teachings of Perlman, Krawczyk, and Taylor in any combination.

Therefore, Applicant believes that independent claims 2, 13, and 18 and their respective dependent claims are distinguishable over the cited prior art references. Accordingly, Applicant respectfully requests the rejection under 35 U.S.C. §103(a) be withdrawn.

Conclusion

Applicant reserves all rights with respect to the applicability of the doctrine of equivalents. Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: June 16, 2008

By /William W. Schaal/
William W. Schaal
Reg. No. 39,018
Tel.: (714) 557-3800 (Pacific Coast)